Support and Rationale Document

for the

Software Communications Architecture Specification

APPENDIX A. USE CASES

15 September 2000

NOTE:

These use cases represent the analysis used during generation of the SCA. They are not a complete set of all possible JTRS use cases, nor are all of the presented use cases complete. Due to the timing of program events, the validation and evaluation of Step 2A and 2B prototypes has replaced the use cases as a source of and/or check on SCA requirements. No further work is planned for these use cases; there are on-going efforts relating to Security use cases which will be included in the SRD.

Revision Summary

1.0	Original release
1.1	Cleanup for release with SRD v1.1

Table of Contents

APPENDIX A USE CASES.

A.1 USE CASE MODELING.

Use case modeling is an object-oriented technique to show the intended functions (use cases) of a system, to show system interaction with external entities (actors outside the system), and to show the relationships between the use cases and actors. Figure A-1 shows the top-level use cases for the SCA-based **Radio System**. At a high level, all capabilities expected of a Radio System implementation fall into one of these use cases. The primary purposes of these use cases and corresponding scenarios are:

1. to describe the functional requirements of the system,
2. to give a consistent description of system capabilities in the form of step-by-step flow of events,
3. to provide a basis for performing system-level tests that verify system functionality, and
4. to provide the ability to trace functional requirements into to-be-developed classes and operations in the system.

A use case model supports system developers in verifying that they develop the right product. A use case model then allows customers and users to validate the system. Use cases do not capture all the requirements of a system. Requirements pertaining to performance, resource usage, and power consumption, are captured as supplementary requirements.

In the following paragraphs, major components of a use case model, which is the general approach for the development of the SCA use case model, and other stages and artifacts of use case analysis are described in detail.

A.1.1 Components of a Use Case Model.

The major components of a use-case model are use cases, actors, and the system to be modeled. An actor is any external entity that has an interest in interacting with the system. Actors may be human actors that initiate a flow of events but can be devices or other systems.

Each use-case in the model describes in detail how the system interacts with the actors, and what the system does in the use case. Use cases are broken down into Scenarios, which are particular instances of the use case. Scenarios are used to identify the classes and interfaces of objects that will perform the functions. They are also used to verify that the design, or architecture, will fulfill the requirements.

A.1.2 Architectural Analysis.

Once the system level requirements have been captured and represented as a use case, architectural analysis is performed. In this phase, analysis mechanisms are applied to define conceptual patterns, a set of analysis classes, and an initial set of layers in the architecture.

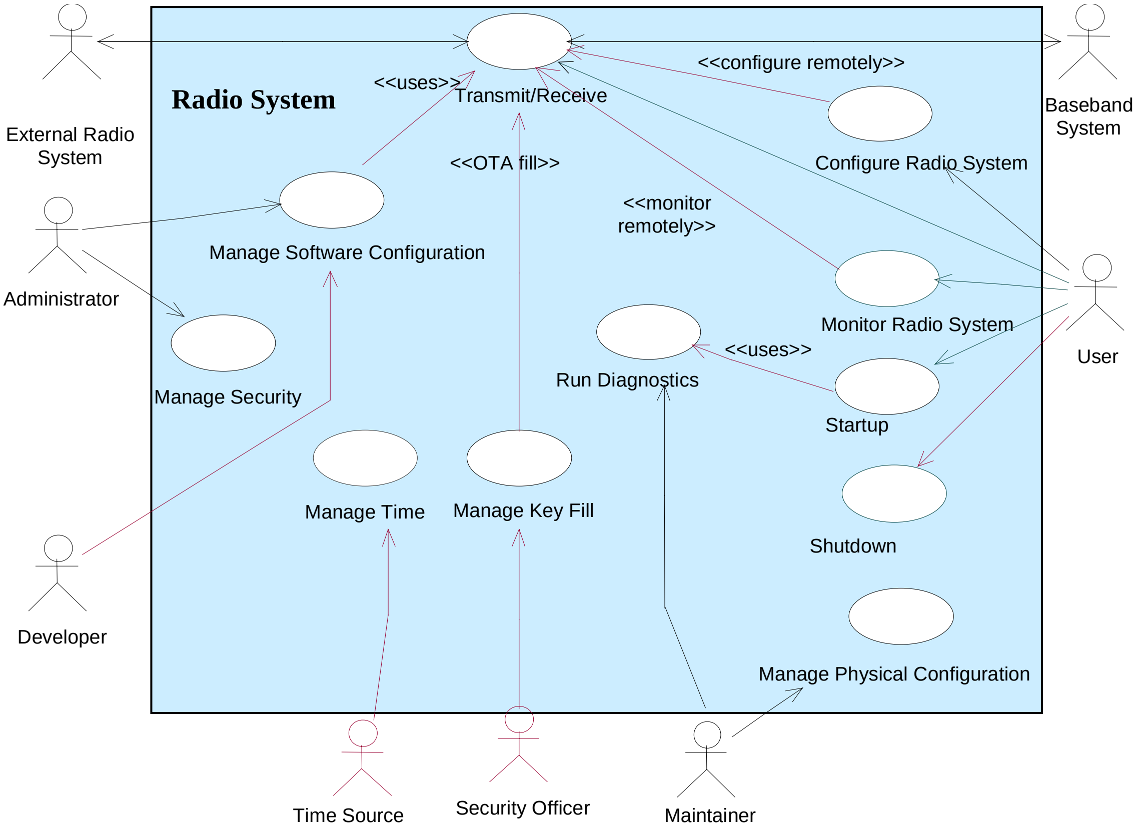

Figure A-1. Use Cases

Analysis mechanisms capture the key aspects of a solution in a way that is implementation dependent. Abstract Classes are key abstractions that are derived from the use case model and are focused on the solution domain. These classes are the starting point for what will eventually be the classes that are part of the architecture definition.

Layers are used to define boundaries between different kinds of services and encapsulate like services.

A.1.3 Use Case Analysis.

In Use Case Analysis the scenarios in the use case are supplemented to include internal behavior. Each use case is then realized (as analysis classes are defined and the internal behavior is allocated to the classes). In addition, the responsibilities, attributes, and associations are defined for each class. This step results in class diagrams and sequence and/or collaboration diagrams that validate the behavior. A sequence diagram describes a pattern of interaction among objects, arranged in a chronological order. Collaboration diagrams emphasize the structural organization of a set of objects that send and receive messages. These diagrams are important artifacts of use case analysis and could be used as a basis for a definition of interfaces in a software architecture.

A.2 USE CASES.

A.2.1 Startup.

A.2.1.1 Power-up and Initialize.

A.2.1.1.1 Brief Description.

An Actor such as the **User**, **Maintainer**, etc., applies power to the **Radio System** which then performs activities such as:

1. BIT/diagnostics
2. Bus enumeration,
3. Communication network configuration
4. I/O configuration
5. Device initialization

The **Radio System** optionally loads default waveform(s) (see note 1).

A.2.1.1.2 Preconditions.

The power is off to the **Radio System** (see note 2)**.** The **User** has authorization to use the **Radio System.**

A.2.1.1.3 Post-conditions.

The **Radio System** is ready to be configured and has optionally established default communications path(s).

A.2.1.1.4 Main Flow.

1	The **User** applies prime power to the **Radio System**.
2a	The **Radio System** successfully completes power-up BIT per the **Run Diagnostics::Initiate System BIT** use case, and the **Radio System** reports status (e.g. OE is operational).
3a	The **User** acknowledges the startup of the OE and begins authorized use of the **Radio System.**
4a	The **Radio System** presents the options for the **User** to **Configure Radio**, **Run Diagnostics**, Receive/Transmit, etc. [end of case]

A.2.1.1.5 Anchored Alternates.

2b	The **Radio System** fails power-up BIT with a critical failure.	
	1	[end of case]
2c	The **Radio System** fails power-up BIT with a non-critical failure.	
	1	The **Radio System** reports failure [continue at 3].
3b	The **User** finds that the operational status is a degraded mode which would not provide sufficient capability for current needs.	
	1	The **User** selects the **shutdown** option. [end of case]

A.2.1.1.6 Floating Alternates.

None.

Note 1: Default waveform boot-up is optionally a function of the **Radio System**, or it may be partitioned out to an application element such as the GUI.

Note 2: The previous **shutdown** of the **Radio System** was performed in an orderly way as per the "**Shutdown**" Use Case. In other cases of more abrupt power-down, separate use case functionality would apply.

A.2.1.2 System Reset

A.2.1.2.1 Brief Description.

This use case begins when the **Radio System** automatically begins to progress through initialization actions after a temporary power loss or after a **User**-requested system reset. The **Radio System** performs initial start-up tasks and configures itself to an operational state as it was established before the reset. This configuration action includes (optionally) loading the waveforms that were loaded at the time of the reset. The **Radio System** then resumes normal operation.

A.2.1.2.2 Preconditions.

The **Radio System** reset is activated or power is resumed after a disruption for a number of seconds**.** The following are available in the **Radio System** non-volatile memory:

1. The list of waveforms that were running or ready to run prior to the reset or power interrupt;
2. The state of the **Radio System** "ReceiveOnly" attribute at the time of the reset or power interrupt;
3. An indication that the previous shutdown was not a result of a **User**-applied commanded shut-down (per Shutdown use case);

A.2.1.2.3 Post-conditions.

The **Radio System** is operational in a configuration equivalent to that before the reset.

A.2.1.2.4 Main Flow.

1	This use case begins when the **Radio System** automatically begins to progress through initialization actions after a temporary power loss or **User**-requested system reset.
2a	The **Radio System** successfully performs all initialization and reconfiguration activities.
3a	The **Radio System** attains operational status and notifies the **User**. [end of case]

A.2.1.2.5 Anchored Alternates.

2b	The **Radio System** notifies the **User** that a subsystem has not successfully re-initialized and requires specific action(s) to proceed.	
	1	**User** corrects the problem and requests continued initialization. [continue at 2a]
2c	The **Radio System** notifies the **User** that a subsystem has not responded to re-initialization and that there are no recovery options.	
	1	**User** acknowledges the failure and initiates fault isolation activity (per **Radio System** Diagnostics use case) or prompt shutdown of primary power if necessary. [end of case]

A.2.1.2.6 Floating Alternates.

None

A.2.1.2.7 Use Case Specific Rules.

None

A.2.2 Manage Security.

A.2.2.1 Define User.

A.2.2.1.1 Brief Description.

The **Administrator** defines a **User** based on an authentication profile and a privilege set. Example privileges include ability to download a waveform, download a new CF, instantiate a waveform, instantiate a CF, execute a key fill, or setup a communication path.

A.2.2.1.2 Preconditions.

The **Administrator** must have logged onto the **Radio System** and been authenticated by the **Radio System** as a valid **Administrator**.

A.2.2.1.3 Post-conditions.

The **Administrator** has completed the definition of a **User**.

A.2.2.1.4 Main Flow.

1	The **Radio System** presents a list of authorized functions for the **Administrator** type**.**
2	The **Administrator** selects Define **User**.
3	The **Radio System** requests username and authentication profile.
4a	The **Administrator** enters the desired username [freeform] and authentication profile [list].
5	The **Radio System** presents a list of authorized privileges for the authentication profile.
6	The **Administrator** selects the desired privilege(s) for the **User**.
	The **Radio System** builds a user identification based on the username, authentication profile and privilege set, then notifies **Administrator** via the HMI that a new **User** has been successfully defined.

A.2.2.1.5 Anchored Alternates.

4b		The **Administrator** provides an invalid username.
	1	The **Radio System** rejects the invalid username. [continue at 3]

A.2.2.1.6 Floating Alternates.

The **Administrator** cancels the function requested. This may be done at any point up to entering the user privileges.

A.2.2.1.7 Access Configuration of Waveform Rules.

The user privileges are defined by the authentication profile for user.

A.2.2.2 Modify User.

A.2.2.2.1 Brief Description.

The **Administrator** chooses to modify a **User**. The modification can include username, authentication profile, or privilege set.

A.2.2.2.2 Preconditions.

The **Administrator** must have logged onto the **Radio System** and been authenticated by the **Radio System** as a valid **Administrator** and a valid **User** is already defined.

A.2.2.2.3 Post-conditions.

The **Administrator** has completed the modification of a **User**.

A.2.2.2.4 Main Flow.

1	The **Radio System** presents a list of authorized functions for the **Administrator** type**.**
2	The **Administrator** selects Modify **User**.
3	The **Radio System** requests username.
4a	The **Administrator** enters the desired username.
5	The **Radio System** presents the defined username and authentication profile in an editable form.
6a	The **Administrator** modifies the username and authentication profile as desired.
7	The **Radio System** presents a list of authorized privileges for the authentication profile.
8	The **Administrator** selects the desired privilege(s) for the **User**.
	The **Radio System** builds a **User** identification based on the username, authentication profile, and privilege set then notifies **Administrator** via the HMI that a new **User** has been successfully defined. [continue at 1]

A.2.2.2.5 Anchored Alternates.

4b		The **Administrator** provides an invalid username.
	1	The **Radio System** rejects the invalid username. [continue at 3]
6b		The **Administrator** provides an invalid username.
	1	The **Radio System** rejects the invalid username. [continue at 5]

A.2.2.2.6 Floating Alternates.

The **Administrator** cancels the function requested. This may be done at any point up to entering the **User** privileges.

A.2.2.2.7 Access Configuration of Waveform Rules.

The user privileges are defined by the authentication profile for user.

A.2.2.3 Delete User.

A.2.2.3.1 Brief Description.

The **Administrator** chooses to delete a **User**.

A.2.2.3.2 Preconditions.

The **Administrator** must have logged onto the **Radio System** and been authenticated by the **Radio System** as a valid **Administrator** and a valid **User** is already defined.

A.2.2.3.3 Post-conditions.

The **Administrator** has completed the deletion of a **User**.

A.2.2.3.4 Main Flow.

1	The **Radio System** presents a list of authorized functions for the **Administrator** type**.**
2	The **Administrator** selects Delete **User**.
3	The **Radio System** requests username.
4a	The **Administrator** enters the desired username.
5	The **Radio System** requests confirmation that the **Administrator** desires to delete the **User**.
6a	The **Administrator** confirms request to delete the designated **User**.
7	The **Radio System** removes the designated **User** identification from the **Radio System User** structure.
8	The **Radio System** notifies **Administrator** of the deletion of the designated **User**. [continue at 1]

A.2.2.3.5 Anchored Alternates.

4b		The **Administrator** provides an invalid username.
	1	The **Radio System** rejects the invalid username. [continue at 3]

A.2.2.3.6 Floating Alternates.

The **Administrator** cancels the function requested. This may be done at any point up to entering the **User** privileges.

A.2.2.3.7 Access Configuration of Waveform Rules.

The user privileges are defined by the authentication profile for user.

A.2.2.4 Lock User.

A.2.2.4.1 Brief Description.

The **Administrator** chooses to lock out a **User** preventing access without deleting.

A.2.2.4.2 Preconditions.

The **Administrator** must have logged onto the **Radio System** and been authenticated by the **Radio System** as a valid **Administrator** and a valid **User** is already defined.

A.2.2.4.3 Post-conditions.

The **Administrator** has completed the lock out of a **User**.

A.2.2.4.4 Main Flow.

1	The **Radio System** presents a list of authorized functions for the **Administrator** type**.**
2	The **Administrator** selects Lock **User**.
3	The **Radio System** requests username.
4a	The **Administrator** enters the desired username.
5a	The **Radio System** requests confirmation that the **Administrator** desires to lock out the **User**.
6a	The **Administrator** confirms request to lock out the designated **User**.
7	The **Radio System** removes the designated **User** identification from the **Radio System** access structure.
8	The **Radio System** notifies **Administrator** of the lock out of the designated user.[continue at 1]

A.2.2.4.5 Anchored Alternates.

4b		The **Administrator** provides an invalid username.
	1	The **Radio System** rejects the invalid username. [continue at 3]
5b		**User** is already locked out
		The **Radio System** notifies the **Administrator** that the designated **User** is already locked. [continue at 3]

A.2.2.4.6 Floating Alternates.

The **Administrator** cancels the function requested. This may be done at any point up to entering the **User** privileges.

A.2.2.4.7 Access Configuration of Waveform Rules.

None.

A.2.2.5 Unlock User.

A.2.2.5.1 Brief Description.

The **Administrator** chooses to restore access to a **User**.

A.2.2.5.2 Preconditions.

The **Administrator** must have logged onto the **Radio System** and been authenticated by the **Radio System** as a valid **Administrator** and a valid **User** is already defined.

A.2.2.5.3 Post-conditions.

The **Administrator** has completed the **User** access restoration.

A.2.2.5.4 Main Flow.

1	The **Radio System** presents a list of authorized functions for the **Administrator** type**.**
2	The **Administrator** selects Unlock **User**.
3	The **Radio System** requests username.
4a	The **Administrator** enters the desired username.
5	The **Radio System** requests confirmation that the **Administrator** desires to restore access to the **User**.
6a	The **Administrator** confirms request to restore access to the designated **User**.
7	The **Radio System** adds the designated **User** identification to the **Radio System** access structure.
8	The **Radio System** notifies **Administrator** of the returned access to the designated **User**. [continue at 1]

A.2.2.5.5 Anchored Alternates.

4b		The **Administrator** provides an invalid username.
	1	The **Radio System** rejects the invalid username. [continue at 3]
5b		**User** is not locked out
	1	The **Radio System** notifies the **Administrator** that the designated **User** is not locked. [continue at 3]

A.2.2.5.6 Floating Alternates.

The **Administrator** cancels the function requested. This may be done at any point up to entering the **User** privileges.

A.2.2.5.7 Access Configuration of Waveform Rules.

None.

A.2.2.6 Detect Physical Tamper.

A.2.2.6.1 Brief Description.

A **User** may attempt to physically tamper with the **Radio System.** The **Radio System** shall implement physical level tampering detection such that a detection of unauthorized cover or access panel removal will cause a security exception.

A.2.2.6.2 Preconditions.

The **Radio System** must be operational.

A.2.2.6.3 Post-conditions.

The **Radio System** has executed a security exception.

A.2.2.6.4 Main Flow.

1	**User** attempts to gain access to the inside of the **Radio System** without entering a special Maintenance mode.
2	**Radio System** detects tamper and executes a security exception.

A.2.2.6.5 Anchored Alternates.

None.

A.2.2.6.6 Floating Alternates.

None.

A.2.2.6.7 Detect Physical Tamper Rules.

None.

A.2.3 Manage Physical Configuration.

A.2.3.1 Install New Hardware Driver(s).

A.2.3.1.1 Brief Description.

The **Maintainer** prepares the **Radio System** for installing a new hardware resource. Upon **Maintainer** request, the **Radio System** will guide the **Maintainer** through the process of installing the necessary drivers. At the end of the dialog, the **Radio System** will bring the new hardware resource up and will start communicating with it by setting up resources that are provided as defined by the Domain profile.

A.2.3.1.2 Preconditions.

The **Maintainer** has been authenticated by the **Radio System** as having the attributes and permissions given to a **Maintainer**. The **Maintainer** has installed new hardware device(s) into the **Radio System** per Hardware Installation Procedures, and powered the **Radio System** per the Startup use case. The **Radio System** will have brought up the main interface option page for the **Maintainer**. Hardware install may require tamper event prior to install. If so, all cryptographic keys will need to be reloaded.

A.2.3.1.3 Post-conditions.

The **Maintainer** has performed the configuration management functions and the **Radio System** will have established communication with the newly installed hardware as well as make its functionality available to the **User**. The **Radio System** returns to the main interface option page for the **Maintainer**.

A.2.3.1.4 Main Flow.

1	**Maintainer** selects Maintain Physical Configuration
2	**Maintainer** selects the option Install New Hardware Device Driver
3a	**Radio System** prompts **Maintainer** to supply software driver(s) for newly installed hardware device(s) and **Maintainer** supplies the software; (Note: **Radio System** attempts automatic detect of driver software but finds none to be applicable.)
4	**Radio System** uses the **Manage Software Configuration::Initiate Local Software Download** to install the software driver
5a	**Radio System** verifies driver configuration and compatibility with the new hardware device
6	**Radio System** uses **Manage Physical Configuration::Determine Co-Site Potential** to establish the probability that this change will cause cosite interference
7a	**Radio System** informs **Maintainer** that the device is ready for use
8	**Radio System** displays the main interface option page for the **Maintainer**

A.2.3.1.5 Anchored Alternates.

3b	**Radio System** detects an existing installed driver for device(s)	
	1	**Radio System** uses **Manage Software Configuration::List Device Drivers** to display existing device drivers and prompts **Maintainer** to select a replacement for the existing driver
	2	[continue at 5]
5b	The **Radio System** requires a reboot to use the new driver	
	1	The **Radio System** informs the **User** that a reboot is required.
	2	The **Maintainer** selects continue
	3	The **Radio System** stores driver installation state information
	4	The **Radio System** reboots [continue at 6]
5c	The **Radio System** is unable to establish communications with the new hardware.	
	1	**Radio System** informs **Maintainer** that the installed hardware resource does not respond
	2	**Maintainer** selects retry [continue at 3] or [end of case]
5d	The **Radio System** determines that the driver configuration or device compatibility is not correct	
	1	**Radio System** informs **Maintainer** that the installed driver is not correct [continue at 3a]
7b	The Co-site potential of the new hardware is deemed unacceptable by the **Maintainer** based on information returned by the **Manage Physical Configuration::Determine Co-Site Potential** use case.	
	1	**Maintainer** selects retry [continue at 3] or [end of case]

A.2.3.1.6 Floating Alternates.

Maintainer may cancel **Manage Physical Configuration** at any time [success]
Maintainer may exit an operation that has stalled at any time [error]

A.2.3.1.7 Install New Hardware Rules.

None.

A.2.3.2 Remove Hardware.

A.2.3.2.1 Brief Description.

The **User** removes are hardware device from the **Radio System.**

A.2.3.2.2 Preconditions.

A.2.3.2.3 Post-conditions.

A.2.3.2.4 Main Flow.

A.2.3.2.5 Anchored Alternates.

A.2.3.2.6 Floating Alternates.

A.2.3.2.7 Remove Hardware Rules.

A.2.3.3 Determine Co-Site Potential

A.2.3.3.1 Brief Description.

The **Radio System** determines the probability for Co-Site interference when a change in physical configuration occurs due to actions of external actor. The **Radio System** will notify the **Maintainer** (and other actors if affected) of this potential interference and provide indication of expected outcome under the condition.

A.2.3.3.2 Preconditions.

The **Maintainer** has been authenticated by the system as having the attributes and permissions given to a **Maintainer**. The **Radio System** has begun to process a physical configuration change request per the Install New Hardware use case.

A.2.3.3.3 Post-conditions.

The **Radio System** notifies the **Maintainer** of a potential co-site interference condition.

A.2.3.3.4 Main Flow.

1	**Radio System** analyzes the requested configuration change and determines that it would cause potential for co-site interference
2	**Radio System** notifies the **Maintainer** of the condition
3a	**Maintainer** selects to continue with the configuration change

A.2.3.3.5 Anchored Alternates.

3b	**Maintainer** selects to abort the configuration change	
	1	**Radio System** aborts the configuration change [end of case]

A.2.3.3.6 Floating Alternates.

Maintainer may direct the **Radio System** to undo the current action [success]
Maintainer may exit an operation that has stalled at any time [error]

A.2.3.3.7 Co-Site Hardware Potential Rules.

None.

A.2.4 Manage Software Configuration.

A.2.4.1 Initiate Local Software Download.

A.2.4.1.1 Brief Description.

The **Radio System** receives a download of new OE or Application software from a local interface and installs or modifies applications on the system accordingly.

A.2.4.1.2 Preconditions.

The **Administrator** has been authenticated by the system as having the attributes and permissions given to an **Administrator**. The **Radio System** brings up the main option interface page for the **Administrator**. Download device is connected to local interface.

A.2.4.1.3 Post-conditions.

The **Radio System** returns to the main option interface page for the **Administrator**.

A.2.4.1.4 Main Flow.

1	**Administrator** selects **Manage Software Configuration**
2	**Administrator** selects option to Install Software
3	**Radio System** displays a list of interfaces for the download
4a	**Administrator** selects a specific download interface from list
5a	**Radio System** successfully establishes communications with the interface
6a	**Radio System** receives the complete download from the device
7a	**Radio System** checks software integrity and authenticates the downloaded software per security rule.
8a	**Radio System** determines that the downloaded software is Application software and performs relevant installation or modification to existing application(s)
9	**Radio System** notifies **Administrator** that application software installation is complete
10	**Radio System** displays the main option interface page for the **Administrator**

A.2.4.1.5 Anchored Alternates

4b	**Administrator** selects the option "File previously loaded" from list	
	1	**Radio System** displays a list of internally stored files ready for installation and **Administrator** selects the file(s) to be installed [continue at 7a]
5b	**Radio System** notifies **Administrator** that communication is not established with the interface and prompts for action(s)	
	1	**Administrator** selects the option *Retry*
	2	[continue at 10]
	3	**Administrator** selects the option *Cancel*
	4	[continue at 10]
6b	**Radio System** notifies **Administrator** that the software download failed to be loaded onto the system and prompts for action.	

	1	**Administrator** selects the option *Quit*
	2	[continue at 10]
	3	**Administrator** selects the option *Repair*
	4	**Radio System** displays type of error and uses **Manage Software Configuration** Scenarios to repair system
	5	[continue at 10]
7b	**Radio System** displays that the security authentication failed	
	1	The **Radio System** logs audit data for failed software download
	2	**Administrator** selects the option *Continue*
	3	[continue at 10]
8b	**Radio System** determines that the downloaded software is Operating Environment Software	
	1	**Radio System** notifies **Administrator** that Operating Environment Software is to be installed or modified
	2	**Administrator** acknowledges and installation begins
	3	**Radio System** completes installation or modification of Operating Environment software
	4	**Radio System** uses Startup::System Reset use case to reboot system
	5	**Radio System** displays load Operating Environment complete
	6	[continue at 10]
10b	**Radio System** fails to install software application	
	1	**Radio System** logs failed install software attempt
	2	[continue at 10]

A.2.4.1.6 Floating Alternates

Administrator may cancel **Manage Software Configuration** at any time [success]
Administrator may exit an operation that has stalled at any time [error]

A.2.4.1.7 Initiate Local Software Download Rules

A.2.4.1.7.1 Download Security Rules

Software downloads are governed by a domain specific security policy.
Radio System logs (to audit database) the source non-repudiation data as required by the security policy.
Radio System provides sink non-repudiation data to **Administrator** as required by the security policy.
Radio System encrypts software files for local storage as required by the security policy.

A.2.4.1.7.2 Domain Registration Rules

All applications are accompanied by an application profile.
Each application profile contains information that describes the application's hardware dependencies.

A.2.4.2 Initiate Solicited OTAP Software Download.

A.2.4.2.1 Brief Description.

The **Radio System** receives data over the air from **External Radio System** and determines that the data contains a solicited software file(s) intended to update/modify **Radio System** functionality. The **Radio System** authenticates the file(s) using means of cryptographic key (i.e., the authentication data accompanies and is cryptographically bound to the transferred file). The **Radio System** stores the received file(s) for software installation. The **Radio System** returns any non-repudiation of receipt data to the **User** if required by the domain specific security policy.

A.2.4.2.2 Preconditions.

The **Administrator** has been authenticated by the system as having the attributes and permissions given to an **Administrator**. The **Radio System** brings up the main option interface page for the **Administrator**.

A.2.4.2.3 Post-conditions.

The **Radio System** has installed files and responds to the initiating system with the status of the operation and the **Radio System** continues with its normal idle operation.

A.2.4.2.4 Main Flow.

1	**Administrator** uses **Radio System** to negotiate with the **External Radio System** to set up for Over The Air Programming(OTAP) file transfer
2a	**Administrator** uses the Configure Radio::Establish Waveform Communication Channel use case to receive subsequent OTAP file(s) over secure (encrypted) communication link.
3a	**Radio System** uses security functions to decrypt, check integrity and authenticate source of the downloaded software per Security Rules.
4a	**Radio System** confirms OTAP file is same as requested file(s) and saves to local storage
5	**Radio System** provides non-repudiation of receipt information to **External Radio System** as required by the domain specific security rule
6	**Radio System** uses **Manage Software Configuration::Initiate Local Software Download** use case to install OTAP received file(s)
7	**Radio System** displays the main option interface page for the **Administrator**

A.2.4.2.5 Anchored Alternates.

2b	**Radio System** does not receive an OTAP within a predetermined timeout interval	
	1	**Administrator** selects the option *Retry*
	2	[continue at 1]
	3	**Administrator** selects the option *Cancel*
	4	[continue at 7]
3b	**Radio System** displays that the security authentication failed	
	1	**Administrator** selects the option *Continue*
	2	**Radio System** logs auditable event as required by the domain specific security policy
	3	[continue at 7]
4b	**Radio System** determines OTAP application filename is not the requested filename	
	1	**Administrator** selects the option *Retry*
	2	**Radio System** logs auditable event as required by the domain specific security policy
	3	[continue at 1
	4	**Administrator** selects the option *Cancel*
	5	[continue at 7]

A.2.4.2.6 Floating Alternates.

External Radio System may cancel Initiate OTAP Software Download at any time [success]

A.2.4.2.7 Initiate Solicited OTAP Software Download Rules.

A.2.4.2.7.1 Download Security Rules

Software downloads are governed by a domain specific security policy.
Radio System logs (to audit database) the source non-repudiation data as required by the security policy.
Radio System provides sink non-repudiation data to **Administrator** as required by the security policy.
Radio System encrypts software files for storage as required by the security policy.

A.2.4.3 Initiate Unsolicited OTAP SW Download.

A.2.4.3.1 Brief Description.

A.2.4.3.2 Preconditions.

A.2.4.3.3 Pre-conditions.

A.2.4.3.4 Post-conditions.

A.2.4.3.5 Main Flow.

A.2.4.3.6 Anchored Alternates.

A.2.4.3.7 Floating Alternates.

A.2.4.4 Transmit OTAP.

A.2.4.4.1 Brief Description.

This use case is applied when a request is received from a remote location via the **External Radio System** to transmit a program via OTAP to that System (solicited case). This use case is also used when the **Maintainer** initiates a transmit to the remote location via **External Radio System** to manage its software configuration (unsolicited case).

A.2.4.4.2 Preconditions.

A.2.4.4.3 Post-conditions.

A.2.4.4.4 Main Flow.

A.2.4.4.5 Anchored Alternates.

A.2.4.4.6 Floating Alternates.

A.2.4.5 Uninstall Application.

A.2.4.5.1 Brief Description.

The **Radio System** upon authenticated command will remove a selected application from the system mass storage in addition to all of the references to the application in any profiles that are kept on the **Radio System**.

A.2.4.5.2 Preconditions.

The **Administrator** must have logged onto the **Radio System** and have been authenticated by the system as having the attributes and permissions given to an **Administrator**. The **Radio System** displays the main option interface page for the **Administrator**.

A.2.4.5.3 Post-conditions.

The **Radio System** has removed the selected application and references to that application and returns the **Administrator** to the main option interface page for the **Administrator**.

A.2.4.5.4 Main Flow.

1	**Administrator** selects maintain software configuration
2	**Administrator** selects option to uninstall an existing software application
3	**Radio System** uses **Manage Software Configuration::List Installed Applications** to display a list of installed software applications to the **Administrator**
4	**Administrator** selects the application to uninstall
5a	**Radio System** requests the **Administrator** for confirmation to perform uninstall action
6	**Radio System** removes the application and all references to that software application from the domain and logs an auditable event as required by the domain specific security policy
7a	**Radio System** displays status of the uninstall action to the **Administrator**
8	**Radio System** displays the main option interface page for the **Administrator**

A.2.4.5.5 Anchored Alternates.

5b	**Radio System** request confirmation to perform action	
	1	**Administrator** selects the option *Cancel*
	2	[continue at 8]
7b	**Radio System** displays that the uninstall option failed	
	1	**Radio System** requests from the **Administrator** whether to retry or quit
	2	**Administrator** selects the option *Retry*
	3	[continue at 6]
	4	**Administrator** selects the option *Quit*
	5	[continue at 8]

A.2.4.5.6 Floating Alternates.

Administrator may cancel Uninstall Software at any time [success]
Administrator may exit an operation that has stalled at any time [error]

A.2.4.5.7 Uninstall Software Rules.

A.2.4.6 List Installed Applications

A.2.4.6.1 Brief Description

The **Radio System** will provide the ability to display a list of applications along with the major attributes that are associated with each application that exists on the system. Managing the application must be done by an **Administrator** that has the proper authority for such actions.

A.2.4.6.2 Preconditions

The **Administrator** must have logged onto the **Radio System** and have been authenticated by the system as having the attributes and permissions given to an **Administrator**. The **Radio System** will have brought up the main interface option page for the **Administrator**.

A.2.4.6.3 Post-Conditions

The **Radio System** has displayed a list of installed applications as required and returns the system to the main interface option page for the **Administrator**.

A.2.4.6.4 Main Flow

1	**Administrator** selects maintain software configuration
2	**Administrator** selects option *List*
3	**Radio System** uses the *File Manager* to provide a list of the software applications on the system
4a	**Radio System** displays a list of Applications that exist on the system. Display includes: Date of install, version, and size
5	**Radio System** displays main option interface page for the **Administrator**

A.2.4.6.5 Anchored Alternates

4b	**Radio System** presents options to the **Administrator**	
	1	**Administrator** selects the option *Quit* [continue at 5]
	2	[continue at 5]
	3	**Administrator** selects an *Application* followed by the option *Detail*
	4	**Radio System** uses the *File Manager* to provide the detailed list of software applications
	5	**Radio System** displays the Application name and software that make up the Application with the attributes: of Version, Size, and any Associations for each of the software application.
	6	**Administrator** selects the option *Continue*
	7	[continue at 5]

A.2.4.6.6 Floating Alternates

Administrator may cancel manage software list applications at any time
Administrator may exit an operation that has stalled at any time

A.2.4.6.7 List Installed Applications Rules

A.2.4.7 List Device Drivers

A.2.5 Run Diagnostics.

A.2.5.1 Enable Background BIT.

A.2.5.1.1 Brief Description.

The **User** directs the **Radio System** to run BIT in the background.

A.2.5.1.2 Preconditions.

Radio is operational and **User** has logged on and been accepted as valid **User**.

A.2.5.1.3 Post-conditions.

Background BIT is running

A.2.5.1.4 Main Flow.

1	**User** requests background BIT.
2a	**Radio** validates that **User** has that privilege and enables background BIT
3a	Background BIT runs.

.

A.2.5.1.5 Anchored Alternates.

2b		**User** does not have the privileges for this function
	1	**Radio** notifies the **User** that he does not have this privilege and exits.
3b		Background BIT detects and reports a failure.
	1	**Radio** logs the failure, reports the failure to the **User** and determines the allowed Modes of Operation in accordance with its Security Policy.

A.2.5.1.6 Floating Alternates.

None

A.2.5.1.7 Enable Background BIT Rules.

The user privileges are defined by the authentication profile for user.

A.2.5.2 Initiate System BIT.

A.2.5.2.1 Brief Description.

The **Maintainer** directs the **Radio System** to run a system level BIT that is possibly destructive.

A.2.5.2.2 Preconditions.

A.2.5.2.3 Post-conditions.

A.2.5.2.4 Main Flow.

A.2.5.2.5 Anchored Alternates.

A.2.5.2.6 Floating Alternates.

A.2.5.2.7 Initiate System BIT Rules.

System BIT is not allowed during a Fill or Software Download operation.

A.2.5.3 Initiate Channel BIT.

A.2.5.3.1 Brief Description.

The **User** directs the **Radio System** to run BIT for a specific radio channel.

A.2.5.3.2 Preconditions.

A.2.5.3.3 Post-conditions.

A.2.5.3.4 Main Flow.

A.2.5.3.5 Anchored Alternates.

A.2.5.3.6 Floating Alternates.

A.2.5.3.7 Initiate Channel BIT Rules.

Channel BIT is not allowed during a Fill or Software Download operation.

A.2.5.4 View Fault Log.

A.2.5.4.1 Brief Description.

The **Maintainer, Administrator, and/or Security Officer** view the fault log produced by BIT.

A.2.5.4.2 Preconditions.

A.2.5.4.3 Post-conditions.

A.2.5.4.4 Main Flow.

A.2.5.4.5 Anchored Alternates.

A.2.5.4.6 Floating Alternates.

A.2.5.4.7 View Fault Log Rules.

A.2.6 Manage Fill.

A.2.6.1 Load Keys.

A.2.6.1.1 Brief Description.

The **Security Officer** shall have the capability to load new keys. The **Radio System** shall require authentication of key information before key load. The **Radio System** shall attempt to authenticate the key fill only once. If the authentication is unsuccessful a security exception shall be generated.

Note: Key load includes a GPS fill.

A.2.6.1.2 Preconditions.

The **Security Officer** must been authenticated as having access to the Load Keys function.

A.2.6.1.3 Post-conditions.

The keys have been successfully loaded or a security exception has been generated.

A.2.6.1.4 Main Flow.

1	The **Radio System** presents a list of authorized functions to the **Security Officer.**
2	The **Security Officer** selects initiate Load Keys option.
3	The **Radio System** instructs the **Security Officer** to attach the **Fill Device** to the **Radio System** fill port and initiates key load.
4a	The **Security Officer** attaches the **Fill Device** to the **Radio System** fill port and initiates key load.
5a	The **Radio System** authenticates the key information.
6a	The **Radio System** loads the key information, logs the load, and sends audit information to fill port.
7	The **Radio System** notifies the **Security Officer** of a successful key load.[end of case]

A.2.6.1.5 Anchored Alternates.

4b		The **Security Officer** does not correctly attach the **Fill Device** to the **Radio System**.
	1	The **Radio System** will not initiate key load and notifies **Security Officer** of problem. [continue at 4a]
5b	1	The **Radio System** fails to authenticate key fill and generates a security exception. [end]
6b		The **Radio System** fails to successfully load the authenticated key fill.
	1	The **Radio System** provides the **Security Officer** with the options to attempt load again or cancel.
	1a	The **Security Officer** selects load again. [continue at 6a]
	1b	The **Security Officer** cancels the key load. [end of case]

A.2.6.1.6 Floating Alternates.

The **Security Officer** may cancel up to selecting fill or when given the option to attempt load again.

A.2.6.1.7 Load Keys Rules.

None.

A.2.6.2 Initiate Software Zeroize of the **Radio System**.

A.2.6.2.1 Brief Description.

The **Security Officer** commands the **Radio System** to erase all its fill information.

A.2.6.2.2 Preconditions.

The **Security Officer** must be authenticated as having access to initiate software zeroize of the **Radio System**.

A.2.6.2.3 Post-conditions.

The **Security Officer** has zeroized the **Radio System** or the **Radio System** has been incapacitated.

A.2.6.2.4 Main Flow.

1	The **Radio System** HMI provides the option to zeroize the **Radio System.**
2	The **Security Officer** selects the Zeroize **Radio System** option.
3a	The **Radio System** zeroizes the **Radio System** and logs the zeroize.
4	The **Radio System** notifies the **Security Officer** of a successful zeroize.

A.2.6.2.5 Anchored Alternates.

3b	The **Radio System** fails to successfully zeroize the **Radio System**.	
	1	The **Radio System** notifies the **Security Officer** of the unsuccessful zeroize and provides the **Security Officer** with the options to attempt zeroize again or cancel..
	2a	The **Security Officer** selects zeroize again. [continue at 3a]
	2b	The **Security Officer** incapacitates the radio. [end of case]

A.2.6.2.6 Floating Alternates.

The **Security Officer** may cancel up to selecting fill or when given the option to attempt zeroize again

A.2.6.2.7 Initiate Software Zeroize of the Radio System Rules.

A software zeroize of the Radio System zeroizes all key information within the Radio System.
Note: An unsuccessful zeroize attempt may result in the box being declared SECRET and handled accordingly.

A.2.6.3 Initiate Software Zeroize of a Specific Waveform.

A.2.6.3.1 Brief Description.

The **Administrator** initiates the erasure of waveform specific information fills.

A.2.6.3.2 Preconditions.

The **Administrator** must been authenticated as having access to initiate software zeroize of a specific waveform(s).

A.2.6.3.3 Post-conditions.

The **Administrator** has zeroized the specific waveform.

A.2.6.3.4 Main Flow.

1	The **Radio System** provides the option to zeroize the specific waveform(s).
2	The **Administrator** selects the specific waveform to zeroize.
3a	The **Radio System** zeroizes the specific waveform and logs the zeroize.
4	The **Radio System** notifies the **Administrator** of a successful zeroize.

A.2.6.3.5 Anchored Alternates.

3b		The **Radio System** fails to successfully zeroize the specific waveform.
		The **Radio System** notifies the **Administrator** of the unsuccessful zeroize.
	1	The **Radio System** provides the **Administrator** with the options to attempt zeroize again or cancel.
	1a	The **Administrator** selects zeroize again. [continue at 3a]
	1b	The **Administrator** selects cancel. [end]

A.2.6.3.6 Floating Alternates.

The **Administrator** may cancel up to selecting fill or when given the option to attempt zeroize again

A.2.6.3.7 Initiate Software Zeroize of a Specific Waveform Rules.

A software zeroize of a specific waveform erases all key information relative to that waveform(s).

A.2.6.4 Initiate Information Fill.

A.2.6.4.1 Brief Description.

The **Security Officer** initiates an information fill.

A.2.6.4.2 Preconditions.

The **Security Officer** must been authenticated with access to initiate information fill.

A.2.6.4.3 Post-conditions.

The **Radio System** has completed an information fill.

A.2.6.4.4 Main Flow.

A.2.6.4.5 Anchored Alternates.

A.2.6.4.6 Floating Alternates.

A.2.6.4.7 Initiate Information Fill Rules.

A.2.6.5 Receive Over the Air Rekey.

A.2.6.5.1 Brief Description.

The **Radio System** receives and authenticates Over the Air Rekey (OTAR) of specific waveform(s) or **Radio System** keys. The transferred keys are stored in the Cryptographic Manager.

A.2.6.5.2 Preconditions.

An encrypted control channel must have already been established.

A.2.6.5.3 Post-conditions.

The specific waveform(s) or **Radio System** keys have authenticated and been stored in the Cryptographic Manager.

A.2.6.5.4 Main Flow.

A.2.6.5.5 Anchored Alternates.

A.2.6.5.6 Floating Alternates.

A.2.6.5.7 Receive OTAR Rules.

A.2.6.6 Receive Over the Air Zeroize.

A.2.6.6.1 Brief Description.

The **Radio System** receives an over the air Zeroize (OTAZ) command from an **External Radio System** to zeroize a specific waveform(s) of the **Radio System**. Due to the nature of the OTAZ command, the command consists of two parts to increase the reliability of accurate execution.

A.2.6.6.2 Preconditions.

An encrypted control channel must have already been established.

A.2.6.6.3 Post-conditions.

The specific waveform(s) of the **Radio System** have been zeroized.

A.2.6.6.4 Main Flow.

1	The **Radio System** receives Part I of an OTAZ command.
2a	The **Radio System** authenticates the **Security Officer** or **User** from the **External Radio System**.
3a	The **Radio System** authenticates the command.
4	The **Radio System** acknowledges the authentication of Part I. (optional depending on command)
5a	The **Radio System** receives Part II of an OTAZ command.
6a	The **Radio System** authenticates the sender of the command.
7a	The **Radio System** authenticates the command.
8	The **Radio System** acknowledges the authentication of Part II. (optional depending on command)
9	The **Radio System** executes the OTAZ.
10	The **Radio System** informs the **User** of the successful execution of the OTAZ.

A.2.6.6.5 Anchored Alternates.

2b		The **Radio System** can not authenticate the sender of the command.
	1	The **Radio System** blocks any further action on this particular reception and logs the attempt with the Part I command.
	2	Part I is NAKed as required.
	3	Information received with Part II is stored with the attempt log for this OTAZ.
	4	Part II is NAKed as required.
3b		The **Radio System** can not authenticate the command.
	1	The **Radio System** blocks any further action on this particular reception and logs the attempt with the Part I command
	2	Information received with Part II is stored with the attempt log.
	3	Part II is NAKed as required.
6b		The **Radio System** can not authenticate the sender of the command.
	1	The **Radio System** blocks any further action on this particular reception and logs the attempt.
	2	Part II is NAKed as required.
7b		The **Radio System** can not authenticate the command.

	1	The **Radio System** blocks any further action on this particular reception and logs the attempt.
	2	Information received with Part II is stored with the attempt log.
	3	Part II is NAKed as required.

A.2.6.6.6 Floating Alternates.

None.

A.2.6.6.7 Receive OTAZ Rules.

The **Transmit/Receive** use case is used to receive the OTAZ Command.
The **Radio System** intercepts and interprets the OTAZ command instead of passing it on to the **Baseband System**.
All fill locations in the **Radio System** are zeroized upon completion of a **Radio System** directed OTAZ
All fill locations associated with a waveform are zeroized upon completion of a waveform directed OTAZ

A.2.6.7 Receive Over the Air Transfer of Keys.

A.2.6.7.1 Brief Description.

The **Radio System** receives and authenticates Over the Air Transfer (OTAT) of **Radio System** keys from an **External Radio System**

A.2.6.7.2 Preconditions.

An encrypted control channel must have already been established.

A.2.6.7.3 Post-conditions.

The **Radio System** keys have authenticated and been stored in the Key Manager.

A.2.6.7.4 Main Flow.

A.2.6.7.5 Anchored Alternates.

A.2.6.7.6 Floating Alternates.

A.2.6.7.7 Receive OTAT Rules.

The OTAT uses the Transmit/Receive use case to receive the OTAT.
The OTAT is intercepted by the Radio and is not passed on to the **Baseband System**.
An OTAT is transparent to the **User** with the transferred keys being stored in the Key Manager.

A.2.6.8 Initiate OTAR.

A.2.6.8.1 Brief Description.

The **Security Officer** shall have the capability to initiate Over the Air Rekey of **Radio System** keys. The transferred keys are stored in the Cryptographic Manager.

A.2.6.8.2 Preconditions.

An encrypted control channel must have already been established.

A.2.6.8.3 Post-conditions.

The OTAR has been initiated.

A.2.6.8.4 Main Flow.

A.2.6.8.5 Anchored Alternates.

A.2.6.8.6 Floating Alternates.

A.2.6.8.7 Initiate OTAR Rules.

A.2.6.9 Initiate OTAZ.

A.2.6.9.1 Brief Description.

The **Security Officer** initiates an Over the Air Zeroize of keys.

A.2.6.9.2 Preconditions.

An encrypted control channel must have already been established.

A.2.6.9.3 Post-conditions.

The OTAZ has been initiated.

A.2.6.9.4 Main Flow.

A.2.6.9.5 Anchored Alternates.

A.2.6.9.6 Floating Alternates.

A.2.6.9.7 Initiate OTAZ Rules.

A software zeroize affects all key information relative to a waveform or the entire **Radio System**.

A.2.6.10 Initiate OTAT.

A.2.6.10.1 Brief Description.

The **Radio System** initiates Over-The-Air-Transfer (OTAT) of **Radio System** keys.

A.2.6.10.2 Preconditions.

An encrypted control channel must have already been established.

A.2.6.10.3 Post-conditions.

The OTAT has been initiated.

A.2.6.10.4 Main Flow.

A.2.6.10.5 Anchored Alternates.

A.2.6.10.6 Floating Alternates.

A.2.6.10.7 Initiate OTAT Rules.

An OTAT is transparent to the user with the transferred keys being stored in the Key Manager.

A.2.6.11 Initiate Algorithm Load.

A.2.6.11.1 Brief Description.

The **Radio System** receives a Cryptographic Algorithm file download. The **Security Officer** executes the load via a fill device attached at the key fill port.

A.2.6.11.2 Preconditions.

Algorithm is encrypted and pre-loaded in a tamper-protected fill device.

The **Security Officer** is authorized to perform the load**.**

Radio System is powered up and operating.

Radio System key fill port is available to accept algorithm download from fill device per the Fill Rule(s) below.

A.2.6.11.3 Post-conditions.

The algorithm download was successfully completed and the **Security Officer** was notified to that effect.

A.2.6.11.4 Main Flow.

1	The **Security Officer** attaches the Fill Device to the **Radio System** Key Fill Port.
2	The **Radio System** recognizes the presence of the Fill Device and configures itself to accept an algorithm load.
3	The **Radio System** indicates to the **Security Officer** (via the Fill Device) that it is ready to receive the download.
4	The **Security Officer** engages the download sequence.
5a	The **Radio System** indicates to the **Security Officer** (via the Fill Device) that the algorithm download was successful.
6a	The **Security Officer** detaches the Fill Device from the Key Fill Port.
7	The **Radio System** recognizes the removal of the Fill device and returns to prior state.

A.2.6.11.5 Anchored Alternates.

6b	Load multiple crypto devices in same session (repeat sequence under control of the Fill Device).	
5b	**Radio System** indicates to the **Security Officer** that download was unsuccessful	
	1	**Security Officer** conducts diagnostics to determine problem.

A.2.6.11.6 Floating Alternates.

None.

A.2.6.11.7 Initiate Algorithm Load Rules.

A.2.6.11.7.1 Fill Rules

Prior to final storage of the algorithm, the Radio System must determine that:

1) the load is authorized

2) the load passes an integrity test (is not corrupted)

A.2.6.11.7.2 Privilege Rules

Person performing the load must be a COMSEC custodian

A.2.7 Configure Radio.

A.2.7.1 Establish Waveform Communication Channel.

A.2.7.1.1 Brief Description.

A **User**-specified waveform is loaded and assigned to a radio channel.

A.2.7.1.2 Preconditions.

The **User** must have been granted access to the system and authorized to establish a communication channel. The waveforms in the list of installed waveforms have been installed per the **Manage Software Configuration** use case.

A.2.7.1.3 Post-conditions.

The waveform is instantiated to a radio channel and is ready for configuration by the **User**.

A.2.7.1.4 Main Flow.

1	The **User** requests that the **Radio System** establish a waveform communication channel.
2a	The **Radio System** presents a list of the installed waveforms in its Domain according to Installed Waveform Rules.
3	The **User** selects a waveform from the list and assigns it to a channel.
4a	The **Radio System** determines that the software resources required to support the waveform are installed in the Domain according to Installed Software rules.
5a	The **Radio System** determines that the devices required to support the waveform are installed in the Domain according to Installed Device Rules.
6a	The **Radio System** determines that the installed devices are currently not allocated to another waveform.
7a	The **Radio System** loads the waveform software onto the allocated devices.
8a	The **Radio System** instantiates the set of resources that comprise the waveform
9	The **Radio System** establishes a communications path utilizing the resources.
10	The **Radio System** checks the integrity of the activated channel and it passes all required tests.
11	The **Radio System** indicates to the **User** that the activated channel is operational and ready for use.[end of case]

A.2.7.1.5 Anchored Alternates.

4b	The software resource(s) are not installed in the **Radio System**'s domain	
	1	The **Radio System** notifies the **User** that the software resource(s) required by the waveform are not installed [continue at 2].
5b	The **Radio System** determines that the required devices are not installed.	
	1	The **Radio System** notifies the **User** that the device(s) required by the waveform are not installed [continue at 2].
6b	The **Radio System** determines that the required devices are currently allocated to another waveform of lower priority.	
	1	The **Radio System** requests confirmation from the **User** that it is acceptable to remove the lower priority communication channel.
	2	The **User** confirms request to preempt.

	3	The **Radio System** performs the de-allocation using **Configure Radio**.
	4	The **Radio System** notifies the **User** that the de-allocation is complete. [continue at 7a]
6c	The **Radio System** determines that the required devices are currently allocated to another waveform of equal or higher priority.	
	1	The **Radio System** notifies **User** that the requested communication channel can not be realized due to resource/device conflicts. [continue at 2.]
7b	The **Radio System** encounters an error when loading the waveform SW.	
	1	The **Radio System** notifies the **User** that an error occurred when loading the waveform SW. [continue at 2]
8b	The waveform instantiation fails (a resource could not be created).	
	1	The **Radio System** notifies the **User** that the load failed [continue at 2].
10a	The **Radio System** checks the integrity of the activated channel and it fails critical test(s).	
	1	The **Radio System** notifies the **User** of the channel failure and prompts the **User** for Retry/Abort.
	2	The **User** aborts.
	3	The **Radio System** cancels events performed thus far in this flow. [end of case]
6b 2b	The **User** aborts the request to preempt. [continue at 2]	

A.2.7.1.6 Floating Alternates.

The **User** can cancel at any time.

A.2.7.1.7 Establish a Waveform Communication Channel Rules.

Installed Waveform Rules

Installed waveforms are represented in the Application Profile.
The characteristics of a waveform are represented in an Application Profile for the waveform.

Installed Software Rules

The software resources required by a waveform are represented in the Resource Profile
The characteristics of a software resource are represented in a Profile for the software resource.

Installed Device Rules

The devices required by the waveform software are defined by the Application Profile for the software application.
The devices installed in the Radio System are represented in the Device Profile.
Device properties are represented in a Device Profile.

A.2.7.2 Set Waveform Parameters.

A.2.7.2.1 Brief Description.

The **User** Actor sets the parameters for an existing waveform on a channel.

A.2.7.2.2 Preconditions.

The waveform must already have been loaded and instantiated with the **Configure Radio::Establish a Waveform Communication Channel** use case.

A.2.7.2.3 Post-conditions.

The waveform is fully configured and is ready for by the **User** Actor in the **Transmit/Receive** use case.

A.2.7.2.4 Main Flow.

1	The **User** selects a **Radio System** channel to configure according to Channel Access Rules.
2	The **Radio System** presents the configuration parameters (frequency, power level, bit rate etc.) of the waveform assigned to the channel to the **User**.
3	The **User** sets one or more of the parameters.
4a	The **Radio System** accepts the parameters and configures the resources accordingly.
5	The **Radio System** indicates to the **User** that the waveform has been configured

A.2.7.2.5 Anchored Alternates.

4b	The **Radio System** rejects the parameter(s)	
	1	The **Radio System** notifies the **User** the parameter(s) have been rejected

A.2.7.2.6 Floating Alternates.

None.

A.2.7.2.7 Set Waveform Parameters Rules.

Channel Access Rules

The **User** is only presented the channels for which the **User** has access rights.

Waveform Parameter Rules

The waveform parameters presented to the user are based on the parameters defined by the application profile of the installed waveform software.
Parameters can be presented as pre-defined configuration sets (presets).
The limits and granularity of each parameter are defined by the application profile for the installed waveform software and cannot be changed by the user.
The Radio System notifies the User if any waveform parameters are not supported by the user interface. The User has the option of disabling this notification.
The Radio System disables any parameters in the user interface that are not supported by the waveform.

A.2.7.3 Determine Cosite Potential.

A.2.7.3.1 Brief Description.

The **Radio System** will attempt to detect any potential of Cosite interference that may exist whenever any information is entered into the system that modifies or adds any selectable component that may aggravate the cosite problems within the system. The **Radio System** will warn the **User** of this potential.

A.2.7.3.2 Preconditions.

The **User** performs an action that causes clock speeds, frequencies, or other R/F related parameters to be changed or added to the system.

A.2.7.3.3 Post-conditions.

The **Radio System** will warn the **User** of the cosite potential and allow the **User** to continue with the desired operation after providing the **User** with the option of undoing the potential problem.

A.2.7.3.4 Main Flow.

A.2.7.3.5 Anchored Alternates.

A.2.7.3.6 Floating Alternates.

User may direct the **Radio System** to undo the current action
User may exit an operation that has stalled at any time [error]

A.2.7.4 Start Waveform.

A.2.7.4.1 Brief Description.

The **User** chooses to start a loaded waveform.

A.2.7.4.2 Preconditions.

The **User** must have been granted access to the system (authenticated).

The waveform must have already been configured by **Configure Radio::Set Waveform Parameters**.

A.2.7.4.3 Post-conditions.

The waveform is started and ready to process communications traffic.

A.2.7.4.4 Main Flow.

1	The **User** selects the waveform channel to start.
2	The **Radio System** signals the waveform resources to allow processing of communications traffic.

A.2.7.4.5 Anchored Alternates.

None.

A.2.7.4.6 Floating Alternates.

None.

A.2.7.4.7 Start Waveform Rules.

The **User** is only presented the waveform channels for which the **User** has access rights.

A.2.7.5 Configure Repeater

A.2.7.5.1 Brief Description.

The **User** instantiates a repeater between two **External Radio System**s.

A.2.7.5.2 Preconditions.

A.2.7.5.3 Post-conditions.

A.2.7.5.4 Main Flow.

A.2.7.5.5 Anchored Alternates.

A.2.7.5.6 Floating Alternates.

A.2.7.5.7 Configure Repeater Rules.

A.2.7.6 Configure Bridge.

A.2.7.6.1 Brief Description.

The **User** instantiates and configures a bridge between two waveforms.

A.2.7.6.2 Preconditions.

A.2.7.6.3 Post-conditions.

A.2.7.6.4 Main Flow.

A.2.7.6.5 Anchored Alternates.

A.2.7.6.6 Floating Alternates.

A.2.7.6.7 Configure Bridge Rules.

A.2.7.7 Configure Router.

A.2.7.7.1 Brief Description.

The **User** configures a router.

A.2.7.7.2 Preconditions.

A.2.7.7.3 Post-conditions.

A.2.7.7.4 Main Flow.

A.2.7.7.5 Anchored Alternates.

A.2.7.7.6 Floating Alternates.

A.2.7.7.7 Configure Router Rules.

A.2.7.8 Configure Gateway.

A.2.7.8.1 Brief Description.

The **User** instantiates and configures a gateway between two waveforms.

A.2.7.8.2 Preconditions.

A.2.7.8.3 Post-conditions.

A.2.7.8.4 Main Flow.

A.2.7.8.5 Anchored Alternates.

A.2.7.8.6 Floating Alternates.

A.2.7.8.7 Configure Gateway Rules.

A.2.7.9 Stop Waveform.

A.2.7.9.1 Brief Description.

The **User** chooses to prevent a waveform from processing communications traffic.

A.2.7.9.2 Preconditions.

The **User** must have been granted access to the system (authenticated).

The waveform must have already been started by **Configure Radio::Start Waveform**.

A.2.7.9.3 Post-conditions.

The waveform is stopped and not processing communications traffic.

A.2.7.9.4 Main Flow.

1	The **User** selects the waveform channel to stop.
2	The **Radio System** signals the waveform resources to stop processing of communications traffic.

A.2.7.9.5 Anchored Alternates.

None.

A.2.7.9.6 Floating Alternates.

None.

A.2.7.9.7 Start Waveform Rules.

The **User** is only presented the waveform channels for which it has access rights.

A.2.7.10 Release Waveform Communication Channel.

A.2.7.10.1 Brief Description.

The **User** chooses to remove an established communication channel.

A.2.7.10.2 Preconditions.

The **User** must have been granted access to the system (logged in).

The waveform must have already been stopped by **Configure Radio::Stop Waveform**.

A.2.7.10.3 Post-conditions.

The channel is removed and the associated resources are freed.

A.2.7.10.4 Main Flow.

1	The **User** selects Release Waveform Communication Channel
2	The **Radio System** presents the **User** with the list of active channels according to Privilege Rules.
3	The **User** selects the waveform channel to release.
4	The **Radio System** disconnects the software resources assigned to the waveform
5a	The **Radio System** disengages the software resources assigned to the waveform
6	The **Radio System** releases the physical resources assigned to the waveform
7	The **Radio System** unloads the waveform software
8	The **Radio System** informs the **User** that the operation is complete.

A.2.7.10.5 Anchored Alternates.

5b	One or more software resources are being used by another waveform channel.	
	1	The **Radio System** does not release those resources [continue at 6].

A.2.7.10.6 Floating Alternates.

None.

A.2.7.10.7 Release Waveform Communication Channel Rules.

Privilege Rules

The **User** is only presented the waveform channels that have been stopped by the Stop Waveform command, and for which it has access rights.

A.2.8 Transmit / Receive.

A.2.8.1 Transmit Voice (non-packet).

A.2.8.1.1 Brief Description.

The **User** wishes to transmit voice over a loaded and configured waveform.

A.2.8.1.2 Preconditions.

The **User** must be authorized to use the **Radio System**. The **User** must have configured the waveform(s) using **Configure Radio::Set Waveform Parameters.**

A.2.8.1.3 Post-conditions.

The voice has been transmitted. The **User** can continue to use the same waveform(s) or select a new one.

A.2.8.1.4 Main Flow.

1a	The **User** is presented with a list of active waveforms by the **Radio System** for which **User** has privilege according to Privilege Rules.
2	The **User** selects the waveform channel(s) to be connected to the **Baseband System.**
3a	The **Radio System** routes audio from the **Baseband System** to the selected waveform channel(s)
4	The **User** requests transmission enable.
5a	The **Radio System** enables transmission(s)
6	The **Radio System** indicates to the **User** that the transmission(s) is enabled.
7	The **Radio System** transmits the audio to the **External Radio System** according to Transmit Rules.
8	The **User** requests transmission disable.
9	The **Radio System** disables the transmission(s).
10	The **Radio System** indicates to the **User** that the transmission(s) is disabled.

A.2.8.1.5 Anchored Alternates.

1b	The **Radio System** is single-channel so the list of active waveforms is not presented.	
	1	[continue at 4]
3b	The **Radio System** is unable to route audio from the **Baseband System** to the selected waveform channel(s).	
	1	The **Radio System** informs the **User** that it is unable to route the audio.
5b	The **Radio System** cannot enable the transmission(s)	
	1	The **Radio System** notifies the **User** of an exception.
	2	[continue at 10]

A.2.8.1.6 Floating Alternates.

The **Radio System** detects the occurrence of a fault (out of lock, over temperature, low output power.)	
1	The **Radio System** disables transmission.
2	The **Radio System** notifies the **User** of the fault.
3	[continue at 10]
The **Radio System** detects an alarm (e.g. Crypto Alarm)	
1	The **Radio System** notifies the **User** of an alarm.

A.2.8.1.7 Transmit Voice (non-packet) Rules.

Privilege Rules

User privilege is domain specific and will be global or restricted based on the platform.

Transmit Rules

SA data transmission will precede audio transmission if selected by **Configure Radio::Set Waveform Parameters**.
The transmission will be secure if selected by **Configure Radio::Set Waveform Parameters**.

A.2.8.2 Transmit Data Stream (non-packet).

A.2.8.2.1 Brief Description.

The **User** wishes to transmit a data stream (e.g. FM data mode: where the data is not in a packet format) over a loaded and configured waveform.

A.2.8.2.2 Preconditions.

The **User** must be authorized to use the **Radio System**. The **User** must have configured the waveform(s) using **Configure Radio::Set Waveform Parameters.**

A.2.8.2.3 Post-conditions.

The data has been transmitted. The **User** can continue to use the same waveform(s) or select a new one.

A.2.8.2.4 Main Flow.

1a	The **User** is presented with a list of active waveforms by the **Radio System** for which **User** has privilege according to Privilege Rules.
2	The **User** selects the waveform channel(s) to be connected to the **Baseband System**.
3a	The **Radio System** routes data from the **Baseband System** to the selected waveform channel(s).
4	The **Baseband System** requests transmission enable.
5a	The **Radio System** enables transmission(s).
6	The **Radio System** indicates to the **Baseband System** and the **User** that the transmission(s) are enabled.
7	The **Radio System** transmits the data to the **External Radio System** according to Transmit Rules.
8	The **Baseband System** requests transmission disable.
9	The **Radio System** disables the transmission(s).
10	The **Radio System** indicates to the **Baseband System** and the **User** the transmission(s) are disabled.

A.2.8.2.5 Anchored Alternates.

1b	The **Radio System** is single-channel so no list is presented	
	1	[continue at 4]
3b	The **Radio System** is unable to route the **Baseband System** interface to the selected waveform channel(s).	
	1	The **Radio System** informs the **User** that it is unable to route the interface.
5b	The **Radio System** cannot enable the transmission(s).	
	1	[continue at 10]

A.2.8.2.6 Floating Alternates

The **Radio System** detects the occurrence of a fault (out of lock, over temperature, low output power.)	
1	The **Radio System** disables transmission.
2	The **Radio System** notifies the **User** of the fault.
3	[continue at 10]
The **Radio System** detects an alarm (e.g. Crypto Alarm)	
1	The **Radio System** notifies the **User** of an alarm. **Verify this is added to all.**

A.2.8.2.7 Transmit Data Stream Rules.

Privilege Rules

Baseband System privilege is domain specific and will be global or restricted based on the platform.

Transmit Rules

SA data transmission will precede data transmission if selected by **Configure Radio:: Set Waveform Parameters**.
The transmission will be encrypted if selected by **Configure Radio::Set Waveform Parameters**.

A.2.8.3 Transmit Packet.

A.2.8.3.1 Brief Description.

The **Radio System** transmits a packet received from the **Baseband System.** The packet may contain data, digitized voice or digitized video.

A.2.8.3.2 Preconditions.

The **Baseband System** must be authorized to use the **Radio System.** The **User** must have configured the waveform using **Configure Radio::Set Waveform Parameters** which may include QoS parameters**.**

A.2.8.3.3 Post-conditions.

The **Radio System** returns to the state it was in before the scenario.

A.2.8.3.4 Main Flow.

1	The **Baseband System** sends a network packet to the **Radio System** according to Network Packet Rules.
2a	The **Radio System** resolves the packet address and routes the packet to the appropriate waveform channel(s).
3	The **Radio System** transmits the packet to the **External Radio System(s)** over the addressed waveform channel(s). according to Transmit Rules

A.2.8.3.5 Anchored Alternates.

2b	The **Radio System** does not have a route for the network address in the packet.	
	1	The **Radio System** drops the packet.

A.2.8.3.6 Floating Alternates.

The **Radio System** detects the occurrence of a fault (out of lock, over temperature, low output power.)	
1	The **Radio System** disables transmission.
2	The **Radio System** notifies the **User** of the fault.
3	[continue at 10]
The **Radio System** detects an alarm (e.g. Crypto Alarm)	
1	The **Radio System** notifies the **User** of an alarm.

A.2.8.3.7 Transmit Packet Rules.

Network Packet Rules

The packet contains a point to point, broadcast or multi-cast address.

Transmit Rules

The transmission will be encrypted if selected by **Configure Radio::Set Waveform Parameters**.

A.2.8.4 Receive Voice (non-packet).

A.2.8.4.1 Brief Description.

The **User** wishes to receive voice data via a loaded and configured waveform.

A.2.8.4.2 Preconditions.

The **User** must be authorized to use the **Radio System**. The **User** must have configured the waveform(s) using **Configure Radio::Set Waveform Parameters.**

A.2.8.4.3 Post-conditions.

The voice data has been received. The **User** is done receiving the voice data via the selected waveform, the **Radio System** is returned to the state it was in before the scenario.

A.2.8.4.4 Main Flow.

1a	The **User** is presented with a list of active waveforms by the **Radio System** for which the **User** has privilege according to the Privilege Rules.
2	The **User** selects the waveform channel to be connected to the **Baseband System** interface.
3	The **Radio System** detects the transmission from the **External Radio System** and provides activity indication.
4a	The **Radio System** routes the audio to the **Baseband System** based on the Receive Rules.
5a	The **Radio System** presents the audio to the **Baseband System**.
6	The **Radio System** detects the end of **External Radio System** transmission.
7	The **Radio System** squelches the output associated with the previous activity and no longer indicates activity.

A.2.8.4.5 Anchored Alternates.

1b	The **Radio System** is single-channel so no list is presented.	
	1	[continue at 3]
4b	The **Radio System** is unable to route the received data to the **Baseband System**.	
	1	The **Radio System** informs the **User** that it is unable to route data to the **Baseband System**.
5b	The **Radio System** is unable to present to audio to the **Baseband System**.	
	1	The **Radio System** informs the **User** that it is unable to present audio to the **Baseband System**.

A.2.8.4.6 Floating Alternates.

The **Radio System** detects the occurrence of a fault (out of lock, over temperature, low output power.)	
1	The **Radio System** disables reception.
2	The **Radio System** notifies the **User** of a fault.
3	[continue at 11]

A.2.8.4.7 Receive Voice Data Rules.

Privilege Rules

User privilege is domain specific and will be global or restricted based on the platform.

Receive Rules

SA will be supported if selected by **Configure Radio::Set Waveform Parameters**.
The transmission will be decrypted if CT is selected by **Configure Radio::Set Waveform Parameters**.
PT transmissions will bypass decryption if CT is selected by **Configure Radio::Set Waveform Parameters**.

A.2.8.5 Receive Stream Data (non-packet).

A.2.8.5.1 Brief Description.

The **User** wishes to receive a data stream (e.g. FM data mode: where the data is not in a packet format) via a loaded and configured waveform.

A.2.8.5.2 Preconditions.

The **User** must have configured the waveform(s) using **Configure Radio::Set Waveform Parameters.**

A.2.8.5.3 Post-conditions.

When the **User** is done receiving a data stream via the selected waveform, the **Radio System** returns to the state it was in previously.

A.2.8.5.4 Main Flow.

1a	The **User** is presented with a list of active waveforms by the **Radio System** for which he/she has privilege.
2	The **User** selects the waveform channel to be connected to the **Baseband System** interface.
3	The **Radio System** detects data and sends the data to the **Baseband system**.
4	The **User** receives entire data stream and the **Radio System** returns to the state it was in previously

A.2.8.5.5 Anchored Alternates.

1b	The **Radio System** is single-channel so no list is presented.	
	1	[continue at 3]
3b	The **Radio System** is unable to route the received data to the **Baseband System**.	
	1	The **Radio System** informs the **User** that it is unable to route data to the **Baseband System** interface.

A.2.8.5.6 Floating Alternates.

None.

A.2.8.5.7 Receive Stream Data Rules.

None.

A.2.8.6 Receive Packet.

A.2.8.6.1 Brief Description.

The **User** wishes to receive packet information (voice, data, or video).

A.2.8.6.2 Preconditions.

The **Baseband System** must be authorized to use the **Radio System.** The **User** must have configured the waveform(s) using **Configure Radio::Set Waveform Parameters** which may include QoS parameters**.**

A.2.8.6.3 Post-conditions.

When the **User** is done receiving data, the **Radio System** returns to the state it was in before the scenario.

A.2.8.6.4 Main Flow.

1	The **External Radio System** sends a transmission that is received by the **Radio System.**
2	The **Radio System** converts the transmission to packet(s).
3a	The **Radio System** resolves the packet addressing and routes the packet(s) to the appropriate **Baseband System(s)**.
4	The **User** receives entire packet transmission and the **Radio System** returns to the state it was in previously

.

A.2.8.6.5 Anchored Alternatives.

3b	**Radio System** determines that the message is addressed to another **User/Radio System** in the routing table.	
	1	**Radio System** determines the next hop to forward message to reach the final destination address.
	2	**Radio System** sends the packet to the next hop in the route to deliver the message to the final destination address.

A.2.8.6.6 Floating Alternates.

None.

A.2.8.6.7 Receive Packet Rules.

A.2.9 Manage Time.

A.2.9.1 Provide System Synchronization.

A.2.9.1.1 Brief Description.

A.2.9.1.2 Preconditions.

A.2.9.1.3 Post-conditions.

A.2.9.1.4 Main Flow.

A.2.9.1.5 Anchored Alternates.

A.2.9.1.6 Floating Alternates.

A.2.9.1.7 Load Waveform Rules.

A.2.9.2 Provide Time to Waveforms.

A.2.9.2.1 Brief Description.

Time is distributed to the waveforms in the **Radio System**.

A.2.9.2.2 Preconditions.

A.2.9.2.3 Post-conditions.

A.2.9.2.4 Main Flow.

A.2.9.2.5 Anchored Alternates.

A.2.9.2.6 Floating Alternates.

A.2.9.2.7 Load Waveform Rules.

A.2.9.3 Synchronize to External Time Source.

A.2.9.3.1 Brief Description.

The **Radio System** is directed to synchronize with an external **Time Source**.

A.2.9.3.2 Preconditions.

A.2.9.3.3 Post-conditions.

A.2.9.3.4 Main Flow.

A.2.9.3.5 Anchored Alternates.

A.2.9.3.6 Floating Alternates.

A.2.9.3.7 Load Waveform Rules.

A.2.10 Monitor Radio System.

A.2.10.1 Provide General Statistics.

A.2.10.1.1 Brief Description.

The **User** accesses general **Radio System** statistics.

A.2.10.1.2 Preconditions.

The **User** must be authorized to use the **Radio System** and be privileged to access general statistics.

A.2.10.1.3 Post-conditions.

The **User** has accessed the desired general statistics and may continue or perform other operations.

A.2.10.1.4 Main Flow.

1	The **User** is presented with a list of functions/statistics by the **Radio System** for which the **User** has privilege to access (view or execute).
2	The **User** selects accessing general statistics.
3a	The **Radio System** supplies general statistics to the **User.**
4	The **User** has completed viewing general statistics and selects termination of the function.
7	The **Radio System** notifies the **User** that the function has been terminated. [Continue at 1]

A.2.10.1.5 Anchored Alternates.

3b	The **Radio System** is unable to retrieve or route the general statistics or the function is not otherwise available	
	1	The **Radio System** notifies the **User** that the requested function is not available.[Continue at 1]

A.2.10.1.6 Floating Alternates.

The **User** elects to cancel the operation	
1	The **User** selects the cancel operation.
2	The **Radio System** request verification of the cancel request.
3a	The **User** verifies request.
3b	The **User** aborts request.
4a	The **Radio System** terminates displaying general statistics [continue at 1].
4b	The **Radio System** continues at the point prior to the **User** selecting the cancel operation.

A.2.10.1.7 Provide General Statistics Rules.

A.2.10.1.7.1 Privilege Rules

User must be authorized to view general statistics.

A.2.10.2 Provide OE Statistics.

A.2.10.2.1 Brief Description.

The **User** obtains **Radio System** Operating Environment (OE) statistics.

A.2.10.2.2 Preconditions.

The **User** must be authorized to use the **Radio System** and be privileged to access OE statistics.

A.2.10.2.3 Post-conditions.

The **User** has obtained the desired OE statistics and may continue or perform other operations.

A.2.10.2.4 Main Flow.

1	The **User** requests and is presented with a list of functions/statistics by the **Radio System** for which the **User** has privilege to access (view or execute).
2a	The **User** selects option to access OE statistics.
3a	The **Radio System** supplies OE statistics to the **User.**
4	The **User** has completed accessing OE statistics and selects termination of the function.
7	The **Radio System** indicates to the **User** that the function has been terminated. [continue at 1]

A.2.10.2.5 Anchored Alternates.

2b	The **User** exits from OE Statistics monitoring	
3b	The **Radio System** is unable to retrieve or route the OE statistics, or the function is not otherwise available	
	1	The **Radio System** notifies the **User** that the requested function is not available[Continue at 1]

A.2.10.2.6 Floating Alternates.

The **User** elects to cancel the operation	
1	The **User** selects the cancel operation.
2	The **Radio System** requests verification of the cancel request.
3a	The **User** verifies request.
3b	The **User** aborts request.
4a	The **Radio System** terminates displaying OE statistics [continue at Main 1].
4b	The **Radio System** continues at the point prior to the **User** selecting the cancel operation.

A.2.10.2.7 Provide OE Statistics Rules.

A.2.10.2.7.1 Privilege Rules

User must be authorized to access OE statistics.

A.2.10.3 Handle Special Monitoring Activity.

A.2.10.3.1 Brief Description.

A.2.10.3.2 Preconditions.

A.2.10.3.3 Post-conditions.

A.2.10.3.4 Main Flow.

A.2.10.3.5 Anchored Alternates.

A.2.10.3.6 Floating Alternates.

A.2.10.3.7 Handle Special Monitoring Activity Rules.

A.2.10.4 Provide Waveform Status.

A.2.10.4.1 Brief Description.

Provide status on an instantiated waveform.

A.2.10.4.2 Preconditions.

A.2.10.4.3 Post-conditions.

A.2.10.4.4 Main Flow.

A.2.10.4.5 Anchored Alternates.

A.2.10.4.6 Floating Alternates.

A.2.10.4.7 Provide Waveform Status Rules.

A.2.10.5 Initiate Alarms.

A.2.10.5.1 Brief Description.

A.2.10.5.2 Preconditions.

A.2.10.5.3 Post-conditions.

A.2.10.5.4 Main Flow.

A.2.10.5.5 Anchored Alternates.

A.2.10.5.6 Floating Alternates.

A.2.10.5.7 Initiate Alarms Rules.

A.2.10.6 Log Historical Data.

A.2.10.6.1 Brief Description.

The alarm condition, warnings and information messages of the registered producers is captured and logged. The logger only logs information while logging state is authenticated by the **Administrator**, **Maintainer** or User. The log level for the producer and consumer is also registered. The log message is based upon log data, current time, log level and producer identification and stores data into log file.

A.2.10.6.2 Preconditions.

The **Administrator**, **Maintainer** or **User** has been authenticated by the **Radio System** as having the attributes and the permissions per security rule. The **Administrator**, **Maintainer** or **User** has authenticated the logging state. The **Administrator**, **Maintainer** or **User** has registered each consumer and producer for logging level.

A.2.10.6.3 Post-conditions.

The **Radio System** returns to the operational condition.

A.2.10.6.4 Main Flow.

A.2.10.6.5 Anchored Alternates.

A.2.10.6.6 Floating Alternates.

A.2.10.6.7 Log Historical Data Rules.

A.2.10.7 View Historical Data.

A.2.10.7.1 Brief Description.

View events and statistics captured by Log Historical Data.

A.2.10.7.2 Preconditions.

A.2.10.7.3 Post-conditions.

A.2.10.7.4 Main Flow.

A.2.10.7.5 Anchored Alternates.

A.2.10.7.6 Floating Alternates.

A.2.10.7.7 View Historical Data Rules.

A.2.11 Shutdown.

A.2.11.1 Loss of Power.

A.2.11.1.1 Brief Description.

The **Radio System** loses power.

A.2.11.1.2 Preconditions.

The **Radio System** is powered on**.**

A.2.11.1.3 Post-conditions.

A.2.11.1.4 Main Flow.

A.2.11.1.5 Anchored Alternates.

A.2.11.1.6 Floating Alternates.

A.2.11.1.7 Loss of Power Rules.

A.2.11.2 Commanded Shutdown.

A.2.11.2.1 Brief Description.

Upon **User**-initiated Shutdown, the **Radio System** automatically performs activities to cleanly prepare **Radio System** for complete power-off event such as:

1. Place hardware devices into proper state for shutdown (per Security Rules for Shutdown).
2. Prompt User to correct invalid states for shutdown
3. Disconnect Communication network(s)
4. Update configuration data in preparation for next Startup (optionally)
5. Provide indication to the User when all waveforms and network connections have been terminated and OE software is in a shutdown configuration
6. Provides option to restart.

A.2.11.2.2 Preconditions.

The **Radio System** is operational per successful Startup.

The **User** has authorization to perform the **Radio System** shutdown.

A.2.11.2.3 Post-conditions.

The **Radio System** is in a shutdown configuration and can be powered off or restarted.

A.2.11.2.4 Main Flow.

1	The use case begins when the **User** issues a shutdown command to the **Radio System**.
2a	The **Radio System** successfully performs all shutdown activities (disconnect communication network(s), etc.) and notifies the **User**.
3a	The **User** acknowledges the shutdown completion and removes primary power from the **Radio System.** [end of case]

A.2.11.2.5 Anchored Alternates.

<table>
<tr><td>2b</td><td colspan="2">The <b>Radio System</b> notifies the <b>User</b> that a hardware subsystem is not in proper shutdown state and requires a specific action to proceed.</td></tr>
<tr><td></td><td>1</td><td><b>User</b> corrects problem and requests continued shutdown [continue at 2]</td></tr>
<tr><td>2c</td><td colspan="2">The <b>Radio System</b> notifies the <b>User</b> that a priority application is in operation and that the <b>User's</b> authorization level does not permit the shutdown. [end of case]</td></tr>
<tr><td>3b</td><td colspan="2">The <b>User</b> initiates a restart.</td></tr>
<tr><td></td><td>1</td><td>The <b>Radio System</b> restarts per the Startup use case. [end of case]</td></tr>
<tr><td>3c</td><td colspan="2">The <b>Radio System</b> shuts itself off (suspends power) [end of case]</td></tr>
</table>

A.2.11.2.6 Floating Alternates.

None.

A.2.11.2.7 Security Rules for Shutdown

During commanded shutdown, the following security rules apply: Store Tables and applications, Erase RED memories and applications, Overwrite RED algorithms, Zeroize RED key, Zeroize all TRANSEC keys;

The architecture must also accommodate shutdown cases of abrupt (intentional or unintentional) power removal. For example, a case maybe made to incorporate internal power supplies to provide hold-up power while software shuts down. When power is abruptly removed, there may be configuration variations that occur upon next power-up, but no damage will occur to the system . Use case scenarios for this would be handled separately.

A.3 USE CASE GLOSSARY

Administrator - An actor on the Radio System that handles security management and software configuration.

ApplicationInstanceTime - The absolute time reference used and managed by an application instance (specifically, a waveform application instance).

ApplicationInstanceTimeOffset - An offset added to RadioSystemTime and conditionally GPSTimeOffset to create ApplicationInstanceTime.

Baseband System - I/O device(s) external to the Radio System associated with the Transmit/Receive capability and exclusive of the User I/O. Examples include laptop, video, picture and voice.

Communication Channel - A chain of communication elements usually associated with an operator-selectable number or a specific hardware set involved in forming a path for information flow. The channel is used in conjunction with the waveform to provide wireless information exchange between operators and/or hosts.

Communication Path - General term for either communication channel or waveform.

Degraded operation - Partial waveform functionality due to a partially failed sub-system(s).

Developer - An actor on the Radio System associated with the management of software configuration.

Domain - A Radio System or Radio Network System applied in a specific operating/communication environment.

GPSTimeOffset - An offset added to RadioSystemTime to create an absolute time value.

NetDeltaTime - An offset added to ApplicationInstanceTime to create OnAirTime. There may be multiple instances of this offset to cover multiple networks.

Notify - To report in such a way that the operator/host (ie. actor) must acknowledge receipt of message.

OnAirTime - This time is representative of any absolute time value used by a waveform for synchronization proposes. Multiple instances of OnAirTime can exist through use of NetDeltaTimeOffset(s).

Operational - Capable of performing all Radio System control functions and running a minimum set of application waveforms in degraded or full-up modes.

Radio Network System - Two or more Radio Systems capable of interacting over wireless network protocol.

RadioSystemFatalTimeEvent - Any event that causes RadioSystemTime to be invalid (power failure, tolerance fault).

RadioSystemTime - A free running time source that can not be modified by software.

Report - To present and/or log information regarding an event, task status, mode of operation, etc.

Radio System - One or more radio communication channels in a wire-connected environment containing at most one Domain Manager, optionally including over-the-air and wire-line networking capabilities, and capable of supporting waveform applications.

RadioSystemTimeOfDayOffset - An offset added to RadioSystemTime and conditionally GPSTimeOffset to create TimeOfDay.

TimeEvent - Any event which modifies a time property used by an application.

TimeOfDay -This time is representative of any absolute time value accessible by a user and/or application. TimeOfDay is maintained by the CF.

Time Source - An actor on the Radio System associated with managing time with the system.

UML - Unified Modeling Language, a standard notation for object oriented development supported by the Object Management Group (OMG).

Use Case - A well-defined functionality within a system or sub-system that interacts with or is associated with other functionalities. A use case is represented as a bubble with an action-oriented name in UML use case diagrams.

Use Case Scenario - An instance of a use case in the form of step-by-step flow through the function(s).

User - An actor on the Radio System that interfaces to a Radio System communication port independent from the baseband system to perform functions of Radio System configuration, monitoring, control, etc. This actor is typically a host computer in the communication domain.

Waveform - A chain of communication elements usually associated with wireless protocol and a software-controlled channel implementation.